NATIONAL DEFENSE UNIVERSITY
STRATEGIC FORUM
INSTITUTE FOR NATIONAL STRATEGIC STUDIES
Number 28, May 1995

What Is Information Warfare?

Author: Martin C. Libicki, Senior Fellow

Note:

Conclusions

Background For This Discussion

DISCUSSION

Is Information War (IW) a nascent, perhaps embryonic art, or simply the newest version of a time-honored feature of warfare? Is it a new form of conflict that owes its existence to the burgeoning global information infrastructure, or an old one whose origin lies in the wetware of the human brain but has been given new life by the information age? Is it a unified field or opportunistic assemblage?

Since March 1993, Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30 (MOP 30) has set forth definitions and relationships that have guided the joint community in its thinking about the related concepts of information warfare and command and control warfare. As these seminal ideas have evolved, their definitions and relationships have changed as well. MOP 30 is under revision, and both higher level policy documents for the Department of Defense and doctrinal publications of the Joint Staff and Services are either in draft form or under revision.

In light of the unformed state of these concepts, alternative definitions and taxonomies for twenty-first century warfare are proposed:

1. command-and-control warfare [C2W];
2. intelligence-based warfare [IBW];
3. electronic warfare [EW];
4. psychological operations [PSYOPS];
5. hackerwar software-based attacks on information systems;
6. information economic warfare [IEW] war via the control of information trade; and
7. cyberwar [combat in the virtual realm].

To appreciate each on its own merits, the centerfold figure defines each form, lists their subforms, and assesses their use as weapons of war.

What Is Information Warfare?(Graphic Illustration)

Certain aspects of IW are as old as history: striking at the enemy's head, deception of all sorts, and psychological operations in general. Others, notably electronic warfare, reached prominence in World War II. The more recent automation of the command center has created more vulnerable targets reachable via iron bombs, and, against penetrable systems, through malevolent software. If societies evolve in the virtual dimension, the significance and frequency of hackerwar against civilian systems, economic information war, and cyberwar would be greatly increased. Psychological operations would also be greatly transformed.

Will Information War prove to be America's sword or a paper mach, shield? The U.S. military clearly profits more from information systems than others do; it also understands their weaknesses better. Both provide a decided edge at information-based warfare, electronic warfare, and command-and-control warfare. We also know information media. However, the United States, within and beyond the military, is also far more dependent than others on information systems. Thus we are more vulnerable to hackerwar and cyberwar. Our culture may be spreading overseas, but that success makes it harder for us to speak to other cultures in their own language.

With information war embracing so many disparate activities, few generalizations cover the entire field. However, three themes recur:

- One side's information systems may be better (more powerful, robust, and reliable) than another's. Yet, information dominance is not like naval dominance where one side's fleet can keep the other bottled up (although information dominance can support dominance in specific physical media). With rare exceptions (e.g., jamming, competition for media share), information is not a zero-sum enterprise. Mastery of IW does not preclude an adversary from doing the same. We cannot suppress its progress.
- Forming an information corps to conduct information warfare should not be undertaken until the corpsmen understand that their primary purpose in life is not to fight their counterparts on the other side.

- Information war is extremely difficult to conduct without precise and reliable knowledge of the other side's architecture: from how news and information media influence its decisions, to the bureaucratic structure of command, to a nation's communications infrastructure, and even to the details of their information systems' software.

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: What is Information Warfare?

B. DATE Report Downloaded From the Internet: 10/03/01

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **National Defense University Press**
Institute for National Strategic Studies
Washington, DC 20001

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 10/03/01**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.